CLAIMS

What is claimed is:

1. A method used for encryption, the method comprising the steps of:
receiving a first digital input from a set of possible digital inputs;
wherein each digital input in said set of possible digital inputs causes a first integrated circuit to generate a corresponding unique output value;
generating a first output value based on applying said first digital input to said first integrated circuit; and
generating a first encryption key based on the first output value.

2. The method of claim 1, wherein the step of generating a first output value is based on anomalies of said first integrated circuit.

3. The method of claim 2, wherein said anomalies are either inherit or intentionally induced.

4. The method of claim 1, wherein:
the steps further include generating a second output value based on applying a second digital input from a second integrated circuit; and
the step of generating a first encryption key based on the first output value includes generating a first encryption key based the first output value and the second output value.

5. The method of claim 4, wherein said second digital input is generated based on said first output value.

6. The method of claim 1, wherein the steps further include
generating a data structure that includes encrypted data encrypted using said first encryption key.

7. The method of claim 6, wherein the steps further include:
causing said first digital input to be stored in persistent storage;
causing said first digital input to be retrieved from said persistent storage;
regenerating said first output value by causing said first digital input to be applied to said first integrated circuit;
regenerating said first encryption key based on said first output value; and
decrypting said encrypted data using said first encryption key.

8. The method of claim 4, wherein the steps further include
generating a data structure that includes encrypted data encrypted using said first encryption key.

9. The method of claim 8, wherein the steps further include:
causing said first digital input to be stored in persistent storage;
causing said first digital input to be retrieved from said persistent storage;
causing said first digital input to be applied to said first integrated circuit to generate said first output value;

regenerating said second digital input based on said first digital input;

regenerating said second output value by applying said second digital input to said second integrated circuit;

regenerating said first encryption key based on the second output value; and

decrypting said encrypted data using said first encryption key.

10. The method of claim 1, wherein the steps further include:

generating a first data structure that contains first data and encrypted first data, wherein said encrypted first data is an encrypted version of said first data encrypted using said first encryption key;

causing to be stored in persistent storage:

a second data structure that specifies said first digital input, and

linking data that associates said first data and said second data structure.

11. The method of claim 10, wherein the steps further include

receiving said first data;

examining said linking data to retrieve said second data structure;

generating said first digital input based on said second data structure;

regenerating said first output value based on applying said first digital input to said first integrated circuit;

regenerating said first encryption key based on the regenerated first output value; and

decrypting said encrypted first data using said first encryption key.

12. The method of claim 10, wherein said first data comprises an identifier value that identifies an attribute associated with said first integrated circuit.

13. The method of claim 12, wherein said identifier value specifies the identity of an entity into which the first integrated circuit has been incorporated.

14. The method of claim 12, wherein said identifier value specifies the ownership of an entity into which the first integrated circuit has been incorporated.

15. A device, the device comprising

a digital input mechanism that applies a first digital input from a set of possible digital inputs, wherein each digital input of said set of possible digital inputs causes an integrated circuit to generate a corresponding unique output value;

an output value detection mechanism that detects a first output value generated based on applying said first digital input to said first integrated circuit; and

a key generation mechanism that generates a first encryption key based on the first output value.

16. The device of claim 15, wherein said output value detection mechanism detects said first output values based on anomalies of said integrated circuit.

17. The device of claim 15, wherein said anomalies are inherent or intentionally induced.

18. A device, the device comprising

means for applying a first digital input from a set of possible digital inputs, wherein each digital input of said set of possible digital inputs causes an integrated circuit to generate a corresponding unique output value;

means for detecting a first output value generated based on applying said first digital input to said first integrated circuit; and

a key generation mechanism that generates a first encryption key based on the first output value.

19. The device of claim 18, wherein said output value detection mechanism detects said first output value based on anomalies of said integrated circuit.

20. The device of claim 18, wherein said anomalies are inherent or intentionally induced.

21. A computer-readable medium carrying one or more sequences of instructions for encryption of information, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving a first digital input from a set of possible digital inputs;

wherein each digital input in said set of possible digital inputs causes a first integrated circuit to generate a corresponding unique output value;

generating a first output value based on applying said first digital input to said first integrated circuit; and

generating a first encryption key based on the first output value.

22. The method of claim 1, wherein the step of generating a first output value is based on anomalies of said first integrated circuit.

23. The method of claim 2, wherein said anomalies are either inherit or intentionally induced.